# TRANSMITTAL SLIP / NOTE D'ENVOI

| To / À | Classification |
|---|---|
| Dirco 2016.11.24 | TS// |
| **From / De** | **File / Dossier** |
| ADP sto Nov. 22 16 | 374-41 (DMNS) |
| **Drafting officer / Rédacteur** | **Date** |
| | 2016 11 21 |

**Subject / Sujet**

**BACKGROUND NOTE FOR DM NATIONAL SECURITY COMMITTEE (24 November 2016)**

| Action / Donnez suite | Priority / Priorité | Deadline / Délai |
|---|---|---|
| ☐ Signature<br>☐ Comments / Commentaires<br>X Approval / Approbation<br>☐ Information | ☐ Routine<br>X Urgent<br>☐ Immediate / Immédiate | 2016 11 22<br>(DIR) |

| Record of Consultation/Approval<br>Rapport de consultation/d'approbation | Consulted<br>Consulté | Concur<br>D'accord<br>Yes<br>Oui | Concur<br>D'accord<br>No<br>Non | Comments / Commentaires |
|---|---|---|---|---|
| DDO Sec | X<br>X<br>X<br>X<br>X<br>21 Nov 16<br>22 Nov 16 | ✓ | | Enclosed are materials in support of your participation at the Deputy Minister Committee on National Security on 24 November. |

CSIS / SCRS
NOV 22 2016
#25513
DIR

CSIS / SCRS
1669
NOV 22 2016

CSIS / SCRS
NOV 22 2016
25513
ADP / DAP

# DEPUTY MINISTERS' COMMITTEE ON NATIONAL SECURITY

**November 24, 2016**

**2:00 p.m. – 3:00 p.m.**

**Langevin Block**

**84 Wellington Street**

# A View on Mega Trends

**(Abridged Version)**

## Abstract

The pace of scientifically driven change across key sectors is accelerating. Many of these evolving technologies interact and may also be interdependent. The rate and impact of technological advances and interactions are often misunderstood or underestimated. Organizations—faced with time, money and people constraints—will struggle to make effective planning and investment decisions. Meant as a backdrop for CSE senior decision makers, this paper aims to provide insights into the interconnected nature of key technology, economic and societal trends across a range of sectors. While these "mega trends" have been considered in the context of Canada's cryptologic mission, other departments and agencies are also likely to be affected by their introduction, adoption and evolution.

## Introduction

The future will continue to be shaped by the convergence of technology advance, financial, political, societal decisions, demographics, as well as unanticipated man-made and natural crises. In the wake of recent financial recessions and terrorist acts, we may be predisposed to consider the future in a negative context. History, however, has proven that societies are resilient and that economic bust cycles are temporary, almost always followed by a boom cycle triggered by new ideas and innovation (e.g. Roaring Twenties, Silent Generation's bull market (1950/1960s), Boomer's boom (1980/1990s), Gen X's bubble and bull market (2000s)). This diagnostic paints a future where the next anticipated cycle will be spurred by the millennial generation who, raised in a technically rich environment, have the potential to launch the next industrial revolution and create an economic boom rivaling—if not surpassing—the one created by the outgoing Boomers.

Against this assumption, this document considers the following mega trends over the next five to fifteen years in the context of a preferred future:

- The Coexistence of Security, Privacy and Trust for On-line Activity;
- The Evolution of the Canadian Economy Toward Knowledge-Based Sectors;
- The Advent of Blockchain Technology and Cryptocurrency;
- The Fourth Industrial Revolution, including Artificial Intelligence;
- The Rise of Millennials and Aging Boomers;
- The "New Normal" of Ubiquitous Encryption; and
- The Rise of Quantum-Related Technologies.

The preferred news headlines presented at the end of each section are illustrative only and do not represent current or proposed policy outcomes.

## Trend 1: The Coexistence of Security, Privacy and Trust for On-line Activity

Renewed dialogue on privacy and security has been spurred by recognition of the vulnerability of on-line communications. Increasingly, mainstream media is reporting on cyber threat activities directed against individuals, governments and critical infrastructure. Unauthorized disclosures of intelligence activities, private sector monitoring, leaks of personal information through corporate data breaches, identity and intellectual property theft, ransomware and other cybercrimes have all contributed to a growing public consciousness of the need for cyber security. This growing awareness has also been driven by the widespread adoption by Canadians of digital and increasingly connected technologies. The ubiquity and capacity of technology have created an environment where vast amounts of personal and otherwise valuable corporate data and intellectual property are, by default, stored on-line.

Various aspects of personal security are becoming more mainstream concepts and increasingly accessible through on-line services and applications. **On-line anonymity** is achieved when one's real identity remains hidden, for example, by using The Onion Router (TOR) or low attribution networks, obfuscating IP addresses, or paying for on-line services with a cryptocurrency (e.g., Bitcoin). **On-line privacy** is achieved by having the means to protect activity, information and data, and prevent it from being accessed by others; this can be achieved by using end-to-end (e2e) encryption, virtual private networks (VPNs), and through legislation and policies for strong data protection. Other protection mechanisms, such as "differential privacy technology" already in use by companies such as Apple and Google, aim to gather data and analyse usage patterns without compromising privacy.

An emerging awareness of the cyber threat, coupled with the increased adoption of digital connected technologies have precipitated the broad availability of commercial encryption products, commercial services and privacy-enhancing technologies for protecting on-line activities with enhanced security, anonymity and privacy. This has prompted debate on how national security and privacy can co-exist, and how trust can be enhanced among technology users, communications service providers and government security and intelligence agencies.

Going forward, the debate over privacy versus national security (e.g. Apple vs. the US Justice Department) is setting the foundation, through the Digital Equilibrium Project, for the creation of a digital constitution led by technology firms, top US national security leaders and privacy advocates. The rule of law should continue to be relied upon to regulate the actions of the state in circumstances where the privacy of individuals may be implicated, despite the fact that technology is having a disruptive influence on this delicate balance. We need to find ways in which technology can address the privacy concerns of the individual without pre-empting the ability of the state to enforce public safety interests, where and as appropriate.

However, security, privacy and trust of the entire community make the technical expertise that can be offered by federal organizations of value in establishing privacy and information security mechanisms that are also technically trustworthy from a cyber-security perspective. The public will look to the government to play a key role in defining standards and building trust in the technology that underpins society and commerce.

**Preferred news headline:** ***"Government of Canada systems ranked best in world for the privacy protection of citizens' information."***

## Trend 2: The Evolution of Knowledge-Based Sectors

Canada's natural resources and energy sectors have been challenged by the recent global recession. The impact of low oil prices can be seen at a macro level through production cutbacks and revenue loss, currency fluctuations and debt levels, and felt among some Canadians through greater personal debt, a higher cost of living, flat wages, and growing challenges in repaying loans and mortgages currently estimated at a collective C$107B.

On the broader financial front, Standard & Poor's Index (S&P) in the US and the TSX in Canada are at the same levels as early 2014. While some economists push for government-sponsored stimulus injections, others are cautioning that markets would benefit by remaining static for the next decade. Among curious emerging trend (Japan, Sweden, and Denmark) is Negative Interest Rate Policies (NIRP), or savings accounts that charge interest and present the potential to distort the financial system, prompt individuals to hoard cash and deal unexpected consequences for the economy.

Looking ahead, world economies that have thrived by relying heavily on the extraction, transformation and use of natural resources, manufacturing plants, transportation, classical banking, are increasingly embracing the power of knowledge-based sectors. This includes leveraging the convergence of information technology and operation technology (IO/OT), financial technologies (FinTech), through automation, innovation, living labs, smart cities initiatives and leveraging clean renewable sources of energy.

In increasingly competitive global market scenarios, states, organizations and individuals will aggressively target emerging expertise and intellectual property belonging to others with a view to prosper or simply keep up with the knowledge economy. This information, most of which will exist beyond government networks in electronic format, will be a highly valuable commodity. Its storage will create new threat vectors to manage and will need to be protected by robust cyber security measures.

**Preferred news headline:** ***"Global enterprise lines up to buy Canadian renewable energy technology."***

## Trend 3: The Advent of Blockchain Technology and Cryptocurrency

Payment processing between a payer, several middle institutions and a recipient has always represented a significant source of revenues for the financial and banking systems. But despite an estimate of $1.7T (trillion) in revenues these systems are considered highly inefficient due to heavy regulations, complex governance models, the number of parties involved, transaction delays, and the rising cost of integrating technology in a centuries-old system. Such inefficiencies have enabled the rapid rise of financial technologies (FinTech).

FinTech is a disruptive and collective line of business featuring companies that use **blockchain** (BC) software to provide financial services via a distributed ledger that maintains a linear, chronological and continuously growing list of data records (blocks) where each block contains information about a transaction and a timestamp linking it to a previous one. Blockchain is designed to record digital transactions in a way that is secure (encryption), reliable, available, distributed, transparent, immutable, irrevocable, auditable, and efficient. Blockchain technology allows people (and machines) who don't

know each other to trust a shared record of events anywhere, anytime. The best known use of blockchain technology is **cryptocurrencies,** such as Bitcoin, Ether and LiteCoin and applications that enable peer-to-peer lending.

Global FinTech investment has already surpassed $12B, with 42 of the world's largest banks in consortia to design and build blockchain solutions. FinTech is not only eroding banks' market shares, but positioning to be the backbone of all transaction-based industries. By simplifying business models, improving efficiency and reducing costs other industries have started to adopt the technology: NASDAQ market exchange pilot, IBM and Samsung proof-of-concept which demonstrate how blockchain can support Internet of Things (IoT) applications, transactions processing and how it can foster coordination among multiple devices.

It is estimated that by 2025, 10% of global GDP will be stored on a blockchain network. While some countries may prohibit the use of blockchain-based cryptocurrencies, China is looking to establish one for routine commerce. Blockchain has much to offer to other industries including retail, supply chains, accounting and auditing, government services, digital identities, health records, electoral systems, real estate and land titles, IoT communications, smart cities, and the protection of critical infrastructures against cyber attacks. Perhaps one of the key challenges, as stated earlier, is that blockchain could allow individuals to function outside an environment governed by policy. Given such challenges, a non-profit open-source development effort called the Hyperledger Project is demonstrating that users should be able to safely share their data using a neutral system instead of keeping it locked away inside private systems. Furthermore, this effort has the longer-term benefit of establishing a trustworthy digital infrastructure that doesn't centralize power with one authority. If done right, blockchain could become the plumbing for all transaction-based systems.

**Preferred news headline:** *"Canada a global FinTech leader with adoption of new secure, blockchain-based cryptocurrency."*

## Trend 4: The Fourth Industrial Revolution

While cyberspace and social media have grabbed global headlines in recent years, a major technology cluster will have an even more seismic impact in coming decades: the Fourth Industrial Revolution (4IR). The 4IR is composed of developments in **artificial intelligence, cognitive technologies, advanced robotics, nanotechnology, augmented and virtual reality, additive manufacturing (3D-4D printing), Industrial Internet of Things, biotechnology, genetics, and augmented humans (neuro and bionics).** We are just at the beginning of the 4IR and these technologies will build on and amplify one another to allow for exponential innovation, development and growth.

The future of **artificial intelligence (AI)** can be broken down into three main categories: 1) **Narrow Intelligence** which seeks to execute specialized tasks such as speech recognition, conversation platforms (chatbots), the execution of specific tasks from managing calendars to controlling IoT devices, etc. Current examples include virtual private assistant such as Siri, Cortana, Alexa, Viv and Now; 2) **Artificial General Intelligence** or AI that's at least as intellectually capable as a human which aims to replicate many aspects of human cognition (2030-2040); and 3) **Artificial Super Intelligence**, the singularity or AI that is smarter than any human (2045-2060). Known for its performances on the television game show *Jeopardy!*, IBM's AI platform Watson has recently been 'hired' by the law firm Baker & Hostetler to handle their bankruptcy practice. Built on IBM's cognitive computer, the Watson Ross program is

considered to be the world's first AI attorney. IBM has also partnered with Softbank to explore the use of robot assistants in retail stores across the US. Other robotic initiatives include: the use of robot assistants to provide product information in Nestle cafés in Japan; and Lowe's and Best Buy in the US have robots that bring merchandise to customers who make a request via a touch screen. These examples show robotics with advanced machine decision making used in domains, until now, exclusively run by humans. Along those lines, the World Economic Forum (WEF) speaks to the possibility of AI sitting on a corporate board of directors within the next decade.

Ubiquitous **cognitive technologies (CT)** will play an increasing crucial role by leveraging: machine learning (systems that can improve their performance without the need to follow programmed instructions); and natural language processing (machines that can process text, extract meaning and generating text like a human, as well as speech recognition, and the ability to automatically and accurately transcribe speech). Successfully integrating CT will improve core functionality, automation and the ability to generate new knowledge. CT may well help in fulfilling the 1.5 million open cyber security jobs projected to be required by 2020 by which time we can expect the majority of the world's largest enterprise software companies to feature integrated CT.

The digital world is increasingly bleeding into the physical world. **Augmented and virtual reality** are taking lessons from the gaming industry and applying them to business (e.g., training and education, data visualization, healthcare diagnostics, product demos, remote assistance, etc.). Digital can also now transition to the physical world through the use of additive manufacturing (i.e. 3D-4D printing). This technology will provide speed advantages in the ability to design, manufacture and test parts, thus avoiding long production cycles, and will have an impact on economies around the world.

The **Industrial Internet of Things (IIoT)** will bring device deployment beyond the current concepts of connectivity and remote accessibility. IIoT will be employed by a wide range of enterprises, government services, and municipalities through critical infrastructures and smart cities projects to address relevant business, consumer and public needs. Interoperability will be the biggest commodity and information will be more valuable than the devices themselves. A negative downside to seamless interoperability is the potential—indeed reality—of botnet platforms used in distributed denial of service (DDoS) attacks against critical infrastructure or other targeted on-line services. According to media reports, the heaviest and most sustained investments in IoT technologies are made by China, India, Singapore and South Korea.

The implications across a range of disciplines are exciting and promise to bring profound change. The **biotechnology, genetics, and augmented humans technology** cluster spans wide and deep as research and development are expected to drastically change how we define humanity. With novel objectives of increasing quality of life and life expectancy through genome editing, these technologies will have a significant impact on physical and cognitive capabilities and human-machine divide.

That said, new technologies will bring new actors. These include state-run laboratories, corporate investors, DIY maker groups, terrorists and organized criminals that are competing to harness and leverage these technologies in pursuit of their interests. As a case in point, in order to drive China's future economic development their latest five-year plan (2016-2020) calls for investments in the order of US$40B on science and about US$35B in basic research. Priority areas include: neuroscience, genetic research, quantum communications and computation, clean energy sources, industrial, medical and military robots.

The broader risk implications from these technologies are many: increased susceptibility to cyber-attacks, difficulty in ascertaining attribution, facilitation of advances in foreign weapon (including biological and chemical) and intelligence systems, AI done wrong and related liability issues, breakdown of trust between individuals, the threat of unemployment, and the ability of policy and regulation to keep up.

In the previous three industrial revolutions, human development advancements were likewise profound, but they also precipitated violent transfers of power. As noted in the World Economic Forum's report on this trend, "Technological innovation will continue to influence how conflicts arise, who fights them, where they are fought and how they are settled. Breakthroughs in a range of technologies – from robotics to nanotechnology, artificial intelligence, genome sequencing, human advancements or meta materials – could destabilize security and shift balances of power."

**Preferred news headline:** "*Canada deploys a world-first driverless transportation infrastructure in key urban centres.*"

## Trend 5: The Rise of the Millennials and Aging Boomers

Millennials are considered the **world's smartest and best-educated generation**, representing a quarter of the global population and soon to make up half the workforce in developed countries. Millennials, raised in a technically rich environment, are already influencing our societies, including the development and use of technology, family and work environments, social programs, and the economy.

Millennials are projecting or riding the wave of change and innovation. Uber-like shared economy applications are impacted by the law of supply and demand, are known to generate volatility, create a price race to the bottom, and significantly redefine the term 'independent worker'. It remains to be seen how Millennials will react to having an algorithm as a boss.

Facing adversity in a world heavily shaped by Boomers and Gen X, Millennials see careers, work environments, and family life very differently than previous generations. A recent study by Steelcase found that the best way to ensure employees' engagement is to give them control over where and how they do their work, which may mean liberating them from having to do everything in collaboration with others, from the culture of meetings and potentially distracting open-concept offices.

Going forward, perhaps the most palpable sign of change is the Millennials' ability to impose new rules for the development and use of technologies that enable a transition towards a sharing economy. The best disruptive example is Uber which completely revolutionized the personal transportation industry. But if past events are a sign of ones to come, it is highly likely that even Uber will be forced to adapt its services with the introduction of autonomous vehicles. In the end, Millennials will be the architects of social, political and technological disruption, and organizations must not only prepare to adapt, but also to attract, hire and retain the wired generation that will innovate to shape our future.

**Preferred news headline:** "*Canada's public service riding innovation wave as top employer for Millennials.*"

## Trend 6: The "New Normal" of Ubiquitous Encryption

Encryption products are being adopted at a profound rate and influencing trends that deal with security, privacy and trust. Their rapid development and implementation come in the wake of increasing discussion about privacy protection in the wake of leaks by private sector players or media reporting about government security and intelligence activities. The recent Apple-FBI imbroglio has transformed the privacy debate into an industry vs. government standoff. In March 2016, several technology companies including Amazon, Airbnb, Cisco, eBay, Facebook, Google, LinkedIn, Microsoft, and Twitter came together to publically support Apple in its ongoing encryption dispute with the FBI, seen as a proxy for intrusive state security actors. Privacy advocates and experts alike have publicly committed to develop encryption products that can secure information and stymie most nation state collection capabilities. Most services have already integrated some level of cryptographic features aimed at enhancing security and privacy, usually baked-in, transparent and simple to use, with end-to-end (e2e) encryption now the norm for communications (messaging services, voice, video-conferencing, cloud services, blockchain technology and cryptocurrencies).

But **encryption** is a complex task, based either on **open or proprietary standards**. The science behind open encryption standards has been publicly developed and tested, and is usually considered to be verifiable and trustable. In the case of proprietary technology, however, products are more likely to be the result of rapid prototyping, to use cheaper or **limited hardware components** and to have less robust implementation. Still, foolproof encryption is complicated by the difficulty of controlling and implementing all aspects of a secure, end-to-end environment. The **human factor**--convenience, user friendliness, time-to-market and weak implementation schemes—remains likely to undermine the effectiveness of strong encryption or other security features.

Going forward, the Internet of Things (IoT) promises to complicate the prospects for encryption and security. Hardware limitations from processors, memory, and communications protocols are currently hindering the use, efficiency or interoperabilty of encryption, and the possibility of implementation errors will persist. The development of next-generation encryption algorithms better suited for micro-computing devices may eventually enable the bring-your-own-device (BYOD) practice in the workplace that enables employees to connect to the organizations' network using their own devices.

**Preferred news headline:** *"On-line commerce on the rise due to increased consumer confidence that transactions are private, secure, and trustworthy."*

## Trend 7: The Rise of Quantum-Related Technologies

At the heart of technology is the design and creation of machines. Machines must obey the laws of physics, until recently the predominant underlying theoretical foundation for virtually all of technology. But in the late 20th century, the miniaturization of computers began to produce devices whose physical size approaches that of individual molecules. To understand the behaviour of these devices, engineers have turned to the theory of quantum physics to explain the bizarre and counter-intuitive results of physics experiments involving extremely tiny systems and discovered that machines could be built to perform operations that were considered impossible in the classical sense. Emerging quantum technologies—including **quantum computers (QC), quantum cryptography (Q Crypt), quantum-resistant cryptography (QR Crypt), quantum key distribution (QKD), and quantum**

**communications** — each exploit quantum physics to provide more power and utility than classical technology. This new class of technologies is rapidly moving from the domain of academic research into the world of commercial technological application.

Canada is home to many of the world's most respected researchers and institutions in the quantum space, including: The Perimeter Institute for Theoretical Physics; The Institute for Quantum Computing (ICQ) at the University of Waterloo; Quantum Valley Investments (QVI); The Institute for Quantum Science and Technology at the University of Calgary; The University of Montreal; The Center for Quantum Information and Quantum Control (CQIQC) at the University of Toronto; The National Research Council (NRC) new National Strategy and Quantum Lab; and Vancouver-based D-Wave Systems Inc. and, to some degree, coordinated through the Natural Sciences and Engineering Research Council of Canada (NSERC).

Going forward, while limited prototypes of quantum computers have been demonstrated, the biggest challenge is scalability. Companies like Google are investing heavily in Q Crypt to secure communications and directly compete with Canada's D-Wave offering while at the same time developing QR Crypt algorithms that can safeguard against future QC capabilities (e.g. New Hope algorithm trial). It is generally acknowledged that quantum technology is still 10 to 30 years away from providing the breakthroughs that would bring tremendous advantages from a security and a financial perspective. From another perspective, the advent of quantum computing would deliver the computational power to break all current cryptographic schemes, which threatens to render most of current encrypted communications readable. There is a pressing need to invest in the near term in quantum-related technologies that would both take advantage of the potential economic and security benefits, as well as to continue to safeguard encrypted communications used by the Government, Canadian national infrastructures and Canadians alike.

**Preferred news headline:** *"Canada experiences reverse brain drain as global quantum experts flock to Waterloo, a city referred to as Quantum Valley."*

## Conclusion

Within roughly five to fifteen years, the mega trends presented in this paper are likely—both individually and in combination—to have a profound impact on Canada's economy, society and security. Indeed, these are global trends that will transcend Canada's border and influence the international community. Each of these trends brings promise and challenge, further compounded by the interconnectedness and interdependence of several key technology advances. Significant and sustained leadership, innovation, partnership and investment will be required to navigate the complexity of the problem space, the accelerated pace of change within Canada's finite internal capacity.

Follow on analysis in these and other emerging mega trends should be conducted to identify and validate:

- the level of awareness of emerging and disruptive technologies;
- the risks associated with any related national security implications; and
- priority areas for further work including strategic assets, technologies and knowledge that will provide the foundation for Canada's future security and prosperity.